SECTION 1. GENERAL

1. Introduction. The United States (U. S.) Communications Security (COMSEC) effort is controlled and managed under a separate set of security standards and procedures f ran those which apply to other classified information. The reasons for this are that COMSEC techniques and materials are targets continually sought by hostile intelligence services and because the loss of U.S. COMSEC information and materials can seriously damage the national interest. There is also a significant body of information indicating that TOP SECRET keying material is a high priority target for exploitation by hostile intelligence services and, therefore, it must be af f orded special attention. The procedures relative to TOP SECRET keying material contained in this Supplement do not apply to Nuclear Command and Control COMSEC material which is controlled in accordance with JCS PUB 13, nor to key locally generated for immediate use, but they do apply to locally generated key which is held in physical or electronic form for future use. This Supplement establishes security requirements consistent with national policy established to protect Us. communications as it applies to the private sector.

a. Department of Defense (DoD) COMSEC inf ormation is made available to contractors and their subcontractors under one or more of the following conditions:

(1) When electrical transmission of classified or sensitive unclassified national defense inf ormat ion among contractors, or between contractors and the Government, is required.

(2) When research, development, production or testing of COMSEC equipment or of communications equipment interfacing with COMSEC equipment is being undertaken on behalf of the Government.

(3) When the contractor is required to install, maintain or operate accountable COMSEC equipment in support-of U.S. Government contracts.

b. The Deputy Director for Information Security, National Security Agency (NSA) , his designated representative, or the Secretary or Head of the User Agency, or his designated representative, may establish additional physical safeguards for the protection of classified COMSEC information because of the nature of the item or the conditions under which it is to be produced or used. Such additional requirements shall be made applicable by incorporate ion in the contract or through appropriate notification f rom the contracting off icer and shall be incorporated into the DoD Contract Security Classification Specification (DD Form 254) .

c. Off icial instructions for the operation and installation of cryptosystems provided by the government or acquired by the contractor are not included in this supplement. They will be furnished separately to the contractor.

d. To help contractors and government personnel simplify their search for appropriate information systems security, the National Security Agency publishes The Information Systems Security Products and Services Catalogue quarterly. It is available by subscription f rom the U.S. Government Printing Off ice. This document contains separate lists of five different categories of NSA-endorsed or -evaluated information systems security products and services.

e. The contractor shall include procedures in or prepare a supplement to his Standard Practice Procedures (SPP), required by paragraph 5s, TSM, to cover COMSEC requirements.

2. PURPOSE. The purpose of this Supplement is to establish policies, procedures and responsibilities for the control of COMSEC material furnished to, generated or acquired by U.S. industry. This Supplement covers the safeguarding controls for classified and unclassified COMSEC material and equipment resident at cleared industrial facilities.

3. SCOPE . This Supplement serves as the single authoritative source for cleared industrial facilities engaged in the development, production, testing, or operational use of COMSEC material in support of U.S. Government contracts.

4. DEFINITIONS. For the purpose of this Supplement, the following definitions apply:

a. ACCESS : The ability and opportunity to obtain knowledge of classified or sensitive information, equipment, or other materials; or the ability and opportunity to have unrestricted use, handling, or physical control thereof. The particular requirements for access to different categories of COMSEC materials vary, and are detailed in this supplement and other official documents.

b. ACCOUNTING LEGEND CODE (AL): A numeric code used to indicate the minimum accounting controls required for COMSEC material. (May also be abbreviated ALC.)

c. ACCOUNTING NUMBER: A number assigned to an individual item of COMSEC material to facilitate its handling and accounting (may also be called register number or serial number).

d. ALC : See Accounting Legend Code.

e. ALTERNATE COMSEC CUSTODIAN: The individual designated by proper authority to perform the duties of the COMSEC Custodian during the temporary absence of the COMSEC Custodian.

f. APPROVED CCI COMMERCIAL CARRIER: A commercial carrier certified by the Military Traffic Management Command (lITMC) or the General Services Administration (GSA) as providing “Constant Surveillance Service (CSS)".

g. ATTENDED: Under continuous positive control of contractor personnel authorized for access or use.

h. AUTHENTICATION : A security measure designed to protect a communications system against acceptance of fraudulent transmissions or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual’s eligibility to receive specific categories of information.

i. AUTHORIZED COMPANY COURIER: A duly authorized and trustworthy individual who has been officially designated to transport/carry COMSEC information and, if the material is classified, is cleared to the level of the material being transported.

j. AUTHORIZED VENDOR PROGRAM: A program in which a vendor producing a secure telecommunications or COMSEC product under contract to NSA is authorized by NSA to produce that product in numbers exceeding the contracted require- ments for direct marketing and sale to eligible buyers under conditions set forth in a Memorandum of Understanding between NSA and the producing vendor.

NOTE : Eligible buyers are typically Government organizations or Government contractors. Products authorized for marketing and sale are placed on the Endorsed Cryptographic Products List.

k. AUTOMATED INFORMATION SYSTEM SECURITY: The totality of security safeguards used to provide a defined level of protection to an automated information system and data handled by it.

l. BINDING: The process of associating a specific communications terminal with a specific key.

m. CA: See Controlling Authority.

n. CALL KEY: See Per Call Key.

o. CANISTER: A type of protective packaging for key in punched or printed tape form.

p. CAP : See Contractor Acquired Property.

q. CCEP : See Commercial COMSEC Endorsement Program.

r. CCI : See Controlled Cryptographic Item.

s. CENTRAL OFFICE OF RECORD (COR): A central office which keeps records of all COMSEC material received by or generated within elements subject to its oversight.

NOTE : Usually within a Government department or agency, its duties include establishing and closing COMSEC accounts, maintaining records of COMSEC Custodian and Alternate COMSEC Custodian appointments, performing COMSEC inventories, and responding to queries concerning account management.

t. CERTIFICATION OF ACTION STATEMENT: A statement attached to the Report of a COMSEC audit by which a COMSEC Custodian certifies that all actions have been completed.

u. CERTIFIED INSTALLATION: An installation that has been determined by the government to meet minimum applicable physical and technical security requirements for the installation of COMSEC equipment.

v. CIK: See Crypto-Ignition Key.

w. CLEARED COURIER: A duly authorized, cleared (to the level of the information being transported), and trustworthy person who has been officially designated to transport classified information.

x. CO: See Contracting Officer

y. COGNIZANT SECURITY OFFICE: The Defense Investigative Service Director of Industrial Security having industrial security jurisdiction over the geographical area in which a facility is located.

z. COMMERCIAL COMSEC ENDORSEMENT PROGRAM (CCEP): A program in which cryptographic subsystems and telecommunications equipment using embedded cryptography are developed, produced, and marketed in accordance with formal agreements between individual commercial vendors and the National Security Agency.

NOTE: Formal agreements are in the form of Memoranda of Understanding (MOU) and more comprehensive Memoranda of Agreement (MOA) between NSA and the commercial vendors. Products proposed for the CCEP must satisfy a number of requirements. The product must be of direct and obvious benefit in meeting national security objectives. The company must not be foreign owned, controlled or influenced, as evidenced by completion and satisfactory evaluation of Certificate Pertaining to Foreign Interest (DD Form 441S). It must obtain a facility clearance and be able to meet NSA product assurance survey requirements. After the product is satisfactorily evaluated, it is endorsed by NSA, placed on the Endorsed Cryptographic Products List, and becomes available-for direct marketing and *sale to* eligible buyers.

aa. COMMON FILL DEVICE (CFD): Any one of a family of devices developed to read in, transfer, or store key (e.g., KOI-18, KYK-13).

ab. COMMUNICATIONS SECURITY (COMSEC): Measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications.

NOTE: COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information. See also Telecommunications and Automated Information Systems Security.

ac. COMPROMISE: a. (General) The disclosure of classified data to persons not authorized to receive that data.

b. (Automated Information Systems) A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information may have occurred.

ad. COMPUTER SECURITY (COMPUSEC) : See Automated Information System Security.

ae. COMSEC : The abbreviation for Communications Security.

af. COMSEC ACCOUNT: An administrative entity identified by an account number, responsible for maintaining custody and control of COMSEC material. (See also Primary Account and Subaccount.)

ag. COMSEC ACCOUNT AUDIT: The periodic examination, announced or unannounced, of COMSEC accounts by the appropriate COR.

ah. COMSEC ACCOUNTING: Procedures which document the control of COMSEC material from its origin through destruction or other final disposition.

ai. COMSEC AIDS: All COMSEC material, other than equipments or devices, which assists in securing telecommunications and is required in the production, operation, and maintenance of COMSEC systems and their components. Some examples are: COMSEC keying material and supporting documentation, such as operating and maintenance manuals.

aj . COMSEC CONTRACTOR: A contractor authorized by contract with the U.S. government to produce COMSEC material.

ak. COMSEC CUSTODIAN: The individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material assigned to a COMSEC account. This applies to both primary accounts and subaccounts.

al. COMSEC EQUIPMENT: Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor, and by reconverting such information to its original form for authorized recipients, and equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment includes crypto-equiprnent, crypto-ancillary equipment> and authentication equipment.

am. COMSEC FACILITY: A facility which contains classified COMSEC material.

an. COMSEC INSECURITY: Any occurrence which jeopardizes the security of COMSEC material or the secure electrical transmission of classified or sensitive government information.

ao. COMSEC INVENTORY RECONCILIATION REPORT: A certificate issued by the COR that compares the semiannual inventory of a COMSEC account with the COR's records and identifies any discrepancies noted.

ap. COMSEC MATERIAL: COMSEC aids and hardware which have the purpose to secure telecommunications or to ensure authenticity of such communications.

NOTE : COMSEC material includes, but is not limited to, COMSEC key, CCI, items which embody or describe COMSEC logic, and other items which perform COMSEC functions.

aq. COMSEC MATERIAL CONTROL SYSTEM (CMCS): A logistics system through which COMSEC material marked "CRYPTO" and other COMSEC material is distributed, controlled, and safeguarded.

NOTE: The CMCS consists of all COMSEC Central Offices of Record (CORs), cryptologistic depots, and COMSEC accounts and sub-accounts.

ar. COMSEC MEASURES: All COMSEC techniques used to secure telecommunications or COMSEC material.

as. COMSEC REGISTER FILE: An accounting file containing a record of each COMSEC item accountable by a contractor.

at. COMSEC SUPPORT SERVICES: See Contractor COMSEC Support Services.

au. COMSEC SUPPORT SYSTEM: The documentation, doctrine, keying material, protection, equipment engineering, production, distribution, modification and maintenance of COMSEC material.

av. COMSEC SYSTEM: The combination of all measures intended to provide communications security for specific telecommunications systems, including associated cryptographic, transmission, emission, computer and physical security measures, as well as the COMSEC support system.

aw. COMSEC VENDOR: A contractor authorized to produce and sell COMSEC equipment.

ax. CONFIGURATION CONTROL: The requirement for proper authority to be granted before a modification can be made to system's hardware, firmware, software, or documentation, so that the system is protected against the introduction of improper modification prior to, during, and after systems implementation.

ay. CONTINGENCY KEY: Keying material held for use on a cryptonet under specific operational conditions or in support of specific contingency plans.

az. CONTRACTING OFFICER (CO): Any government official who in accordance with departmental or agency procedures is currently designated as a contracting officer with the authority to enter into and administer contracts and make determinations and findings with respect thereto or any part of such authority.

ba. CONTRACTOR-ACQUIRED PROPERTY (CAP): Property acquired by or otherwise provided to a contractor for performance under a contract and to which the Government has title.

bb. CONTRACTOR COMSEC SUPPORT SERVICES: Services provided at the contractor level including installation, maintenance, keying, etc.

bc. CONTRACTOR-OWNED EQUIPMENT: See Plant Equipment.

bd. CONTROLLED CRYPTOGRAPHIC ITEM (CCI): A secure telecommunications or information handling equipment, or associated cryptographic component or ancillary device which is unclassified when unkeyed (or when keyed with unclassified key) but controlled. Equipments and components so designated shall bear the designator “Controlled Cryptographic Item” or "CCI".

NOTE : Certain non-cryptographic hardware items which perform critical COMSEC functions are also designated "CCI." CCIS may be procured only by government entities and government contractors.

be. CONTROLLED SPACE: An area to which access is physically controlled.

bf. CONTROLLING AUTHORITY (CA): The designated official responsible for directing the operation of a cryptonet.

bg. COR: See Central Office of Record

bh. CRYPTO : A marking or designator identifying all COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive but unclassified government or government-derived information, the loss of which could adversely affect the national security interest.

bi. CRYPTO-ANCILLARY EQUIPMENT: Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but which does not itself perform cryptographic functions.

bj . CRYPTO-EQUIPMENT: Equipment which embodies a cryptographic logic.

bk. CRYPTOGRAPHIC COMPONENT: The hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or automated information processing system. A cryptographic component may be a modular assembly, a printed wiring assembly (PWA), a microcircuit, or a combination of these items.

bl. CRYPTOGRAPHY : The principles, means, and methods for rendering plain information unintelligible to the uninitiated and for restoring encrypted information to intelligible form.

bm. CRYPTO-IGNITION KEY (CIK): A key storage device that must be plugged into a COMSEC equipment to enable secure communications.

bn. CRYPTOMATERIAL : All material, including documents, devices, or equipment that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications.

bo . CRYPTONET: The stations holding a specific short title of operational or contingency key who can communicate with one another.

bp. CRYPTONET COMPARTMENTATION: Limiting cryptonet size as a means of controlling the volume of traffic protected by that key or limiting the distribution of key to specific user communities.

bq. CRYPTOPERIOD: The time span during which each key setting for a cryptoperiod remains in effect.

br. CRYPTOSECURITY : The security or protection resulting from the proper use of technically sound cryptosystems.

bs. CRYPTOSYSTEM: The associated items of COMSEC material used as a unit to provide a single means of encryption or decryption.

bt . CSO : See Cognizant Security Office.

bu . DCS : See Defense Courier Service.

bv . DCS FORM 1: The receipt for material shipped via DCS.

bw. DCS FORM 10: The Defense Courier Authorization Record which authorizes contractor personnel to receipt for DCS shipped material.

NOTE : ARFCOS Forms 1 and 10 may be used until exhausted.

bx . DD250: Material Inspection and Receiving Report.

by. DECRYPTION: A generic term encompassing decoding and deciphering.

bz . DEFENSE COURIER SERVICE (DCS): Formerly ARMED FORCES COURIER SERVICE. The Defense Courier Service was established by Department of Defense Directive 5200.33, dated September 30, 1987. The DCS is a joint military courier organization under the cognizance of the Commander in Chief, Military Airlift Command (CINCMAC). The DCS is authorized to transport all types and classifications of Government materials, including classified cryptographic equipment, and keying materials designated CRYPTO.

ca. DEPOT MAINTENANCE: See Full Maintenance

cb . DESTRUCTION REPORT: Documentation on an SF153 of the physical or electronic destruction of COMSEC material by NSA-authorized means.

cc. DIRECT SHIPMENT: Shipment of COMSEC material directly from NSA to using COMSEC accounts.

cd. DIRNSA: The Director, National Security Agency. Often used as a generalized address for official correspondence with the National Security Agency.

ce. DIS : Defense Investigative Service.

cf . DROP ACCOUNTABILITY: A procedure under which a COMSEC account initially receipts for COMSEC material, and then provides no further accounting for it to its Central Office of Record (COR). AL-4 items are drop accountable.

Cg. ELEMENT : A subdivision of COMSEC equipment, or an assembly or sub-assembly which normally consists of a single piece or group of replaceable parts. An element is a removable item necessary to the operation of an equipment, but does not necessarily perform a complete function in itself.

ch. EMBEDDED CRYPTOGRAPHY: Cryptography incorporated within an equipment or system whose basic function is not cryptographic.

ci. EMISSION SECURITY: The protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment, automated information systems and telecommunications systems.

cj. FAR: Federal Acquisition Regulation.

ck. FILL DEVICE: See Common Fill Device.

cl. FORMAL TRAINING: Classroom and laboratory instruction conducted by qualified instructors using an approved course of instruction and employing a method for determining whether the student meets established performance requirements for satisfactory completion. "On-the-job" training does not meet the intent of this definition.

cm. FORTUITOUS CONDUCTOR: Continuous metallic objects (e.g., water pipes, heating/cooling ducts, ceiling grids, structural steel, etc.) capable of serving as a conduction path for compromising emanations through the controlled space boundary.

cn. FULL MAINTENANCE: Complete diagnostic repair, modification, and overhaul of COMSEC equipment including repair of defective assemblies by piece part replacement.

co. GOVERNMENT CONTRACTOR TELECOMMUNICATIONS: Telecommunications between or among government departments or agencies and their contractors, and telecommunications of, between or among government contractors and their subcontractors, which relate to Government business or performance of a Government contract.

Cp. Government Furnished Property (GFP): Property in the possession of, or directly acquired by the Government, and subsequently made available to a contractor but to which the Government retains ownership. Government Furnished Equipment (GFE) is included in this definition.

Cq. HAND RECEIPT: A document used to record local or temporary transfer of COMSEC material from a COMSEC Custodian to a user and acceptance by the user of the responsibility for the COMSEC material.

cr. HARD-COPY KEY: Physical keying material such as printed key cards/lists, punched key tapes, or programmable, read-only memories (PROMS).

Cs. HARD-WIRED KEY: Key which *is* permanently installed in a COMSEC equipment.

ct. IMITATIVE (COMMUNICATIONS) DECEPTION: Introduction of deceptive messages or signals into an adversary's telecommunications signals.

cu. INDUSTRIAL TEMPEST PROGRAM: A program established to support U.S. manufacturers who wish to produce TEMPEST-suppressed equipment to sell to the U.S. Government. Qualified participants in the program are supplied classified TEMPEST information. Resulting equipment, if accredited, will be listed in the U.S. Government Preferred Products List.

cv. INFORMATION SYSTEMS SECURITY PRODUCTS AND SERVICES CATALOGUE: Published quarterly by the NSA Information Systems Security Organization and available by subscription from the U.S. Government Printing Office (GPO), this document contains five lists which were previously published separately: The Endorsed Cryptographic Products List (ECPL), NSA Endorsed Data Encryption Standard (DES) Products List, Protected Services List, Evaluated Products List, and Preferred Products List.

Cw. INSECURITY: See Cryptographic Insecurity, Personnel Insecurity, and Physical Insecurity.

Cx. INVENTORY: (a) The physical verification of the presence of each item of COMSEC material charged to a COMSEC account. (b) A listing of each item of material charged to a COMSEC account.

Cy. INVENTORY REPORT: A report of items of material that were physically sighted in accordance with inventory procedure.

Cz. IRREGULARLY SUPERSEDED KEYING MATERIAL: Keying material used on an "as-needed" basis, rather than during a specified period of time.

da. ITP: See Industrial TEMPEST Program.

db. KDC: See Key Distribution Center

dc. KEY: Information (usually a sequence of random binary digits) used to initially set up and to periodically change the operations performed in a crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic countermeasures (ECCM) patterns (frequency hopping or spread spectrum), or for producing other keys.

dd. KEY DISTRIBUTION CENTER (KDC): A COMSEC facility that generates and distributes key in electrical form.

de. KEY ENCRYPTION KEY: A key that is used in the encryption and decryption of other keys, for transmission (rekeying) or storage.

df. KEY LIST: A printed series of key settings for a specific cryptonet.

dg. KEY MANAGEMENT: The process by which key is generated, stored, protected, transferred, loaded, and destroyed.

dh. KEYED: The condition of containing key. In applications employing a CIK, the crypto-equipment is considered unkeyed when the CIK is removed.

di. KEYING: All keying-related changes to the crypto-equipment, such as inserting the Crypto-Ignition Key, loading electronic key, and updating or zeroizing key.

dj . KEYING MATERIAL : A type of COMSEC aid which supplies encoding means for manual and automanual cryptosystems or key for machine cryptosystems.

dk . KEYING MATERIAL SUPPORT PLAN: A detailed description of the operational needs of a proposed cryptonet including the structure, keying material specifications, and distribution plan.

dl. KMSP : See Key Management Support Plan.

dm. L6061 : COMSEC Material Record Form which documents facility possession, location, and current user of a specific equipment or device.

dn. LIMITED MAINTENANCE: COMSEC maintenance performed by personnel who are not authorized to know the details of the cryptoalgorithm. Limited maintenance of a crypto-equipment normally involves disassembly, trouble isolation, and replacing faulty subassemblies (without soldering).

do. LONG TITLE: The descriptive title of an item of COMSEC material (e.g., General Purpose Encryption Device).

dp . MAINTENANCE KEY: Key intended only for off-the-air, in-shop, use. Maintenance key may not be used to protect classified or sensitive but unclassified government information.

dq . MASTER DISPOSITION RECORD: An account maintained by the contractor/vendor which itemizes serial numbers of equipments or components and shipping information where applicable.

dr. MODIFICATION: Any change to the electrical, mechanical, or software characteristics of a COMSEC equipment, assembly, or device.

ds . MANDATORY MODIFICATION: A change to a COMSEC end item which NSA requires to be completed and reported by a specified time compliance date.

dt. NEGATIVE INVENTORY: An annual pre-printed inventory sent to a COMSEC account which does not currently hold COMSEC material.

du. NET MODE: A mode of operation in which all net members have the same key.

dv . NET KEY: A key held in common by all members of a given cryptonet.

dw . NET VARIABLE: See Net Key.

dx . NO-LONE ZONE: An area, room, or space to which no person may have unaccompanied access and which, when manned, must be occupied by two or more appropriately cleared individuals.

dy . OPERATIONAL KEY: Key intended for use on-the-air for protection of operational information or for the production of secure electrical transmission of key streams.

dz . PAGE CHECK: Verification of the presence of each required page in a publication.

ea. PDS : See Protected Distributed System.

eb. PER CALL KEY : A key which is generated on demand and distributed electrically to secure an individual time period of communication between or among users authorized that key. Per call key is a type of Traffic Encryption Key (TEK).

ec. PERSONNEL INSECURITY: The capture, unauthorized absence, defection or control by a hostile intelligence entity of an individual having knowledge of, or access to, classified or sensitive COMSEC information or material.

ed. PERSONNEL SECURITY: The procedure established to ensure that all personnel who have access to sensitive or classified information have the required authority as well as appropriate clearance.

ee. PHYSICAL SECURITY: The application of physical barriers and control procedures to prevent unauthorized access to resources, information, or material.

ef. PLANT EQUIPMENT: Contractor property of a capital nature (including equipment, machine tools, test equipment, telecommunications security and protection equipment, furniture, vehicles, and accessory and auxiliary items) .

eg. PPL : See Preferred Products List.

eh. PREFERRED PRODUCTS LIST: A list of commercially produced equipment which meets TEMPEST and other requirements prescribed by the National Security Agency. This list is contained in the Information Systems Security Products and Services Catalogue.

ei. PROTECTED DISTRIBUTION SYSTEM (PDS): A wireline or fiber-optics system which includes adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of classified information.

ej . PROTECTIVE PACKAGING: Packaging techniques for keying material which discourage penetration and/or which reveal that a penetration has occurred, or which inhibit viewing or copying of keying material prior to the time it is exposed for use.

ek. REGULARLY SUPERSEDED KEYING MATERIAL: Keying material which is superseded on a regular established schedule.

el. REINSTALLATION : The connection of previously installed equipment which has been moved to a new location at a facility.

em. REMOTE REKEYING: Secure electrical distribution of a key by radio or wire/fiber optic line.

en. RESERVE KEYING MATERIAL: Key held to satisfy unplanned needs.

eo. SELF-AUTHENTICATION : Implicit authentication of all transmissions on a secure system (such as PDS) or cryptonet to a predetermined level.

ep. SENSITIVE BUT UNCLASSIFIED INFORMATION: Information, the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests.

NOTE : National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens. The heads of Federal Government departments and agencies are responsible for determining what information is sensitive, but unclassified, and for providing systems protection for such information when transmitted, processed or stored in or on telecommunications and automated information systems.

eq. SUPERSESSION: Scheduled or unscheduled replacement of a COMSEC aid with a different edition.

er. SYSTEM CERTIFICATION: The determination that physical and technical security (especially TEMPEST) requirements have been met.

es. TAMPERING: An unauthorized modification which alters the proper functioning of a cryptographic or automated information processing equipment or system in a manner which degrades the security it provides.

et. TEST KEY: Key intended for “on-the-air” testing of COMSEC equipment or systems.

eu. TRAFFIC ENCRYPTION KEY: Key used to encrypt plain text or superencrypt previously encrypted text and/or to decrypt cipher text.

ev. TRAINING KEY: Cryptographic key intended for use for on-the-air or off-the-air training.

ew. TRANSFER OF ACCOUNTABILITY: The process of transferring accountability for COMSEC material from the COMSEC account of the shipping organization to the COMSEC account of the receiving organization.

ex. TWO-PERSON INTEGRITY: A system of storage and handling designed to prohibit access to certain COMSEC keying material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. NOTE : The concept of “Two-Person Integrity” (TPI) procedures differs from “No-Lone Zone” procedures in that under TPI controls, two authorized persons must directly participate in the handling and safeguarding of the keying material (as in accessing storage containers, transportation, keying/rekeying operations, and destruction). No-Lone Zone controls are less restrictive in that the two authorized persons need only to be physically present in the common area where the material is located. Two Person Control refers to Nuclear Command and Control COMSEC material while Two-Person Integrity refers only *to* COMSEC keying material.

ey. UNIQUE KEY: See Key Encryption Key.

ez. UNIQUE VARIABLE: See Key Encryption Key.

fa. UNKEYED: Containing no key or containing key which has been protected from unauthorized use by removing the CIK.

fb. UPDATE: A cryptographic process which is performed to irreversibly modify the key to protect back traffic.

fc. USER: An individual who is required to use COMSEC material in the performance of his official duties and who is responsible for safeguarding that COMSEC material.

fd. VENDOR: See COMSEC Vendor.

fe. VULNERABILITY: A weakness in a telecommunications system, automated information system, or cryptographic system, or system security procedures, hardware design, internal controls, etc., which could be exploited to gain unauthorized access to classified or sensitive information.

ff. WITNESS: An appropriately cleared (if applicable) and designated individual, other than the COMSEC Custodian, who witnesses the inventory or destruction of COMSEC material.

fg. ZEROIZE: To remove or eliminate the key from a crypto-equipment or fill device.

5. Subcontracting:

a. Classified or sensitive unclassified COMSEC information shall not be disclosed to a potential subcontractor nor shall the contractor negotiate or award a subcontract requiring the disclosure of such COMSEC information without the prior written approval of the government contracting officer.

b. When awarding subcontracts which will involve the fabrication of classified or CCI COMSEC material, prime contractors shall require that subcontractors develop in-process accounting procedures and submit them to the NSA COR through the prime contractor for approval. These procedures shall be developed in accordance with the in-process accounting procedures contained in this supplement and shall be submitted to NSA for review a minimum of 90 days prior to the start of fabrication of classified or CCI material. Prime contractors shall require that subcontractors do not commence fabrication of classified or CCI materials until the applicable in-process accounting procedure has been reviewed and approved by the NSA COR. For classified subcontracts, prime contractors shall ensure that the requirements for in-process accounting are specified in the subcontractor's Contract Security Classification Specification (DD Form 254). If the subcontract involves fabrication of an item after it has transitioned to CCI and no classified information is provided to, or no classified test results are generated by the subcontractor, then the in-process requirements will be included in the appropriate contractual document.

6. TEMPEST Countermeasures.

TEMPEST countermeasures are not addressed in this supplement.

7. Foreign Bids and Proposals.

A contractor who is, or who has been, engaged in a COMSEC contract involving information on behalf of a User Agency or contractor facility shall not enter *into discussion nor negotiate* on *matters involving COMSEC information with* representatives of other nations or with representatives of foreign commercial firms, without prior written approval from the User Agency or the Deputy Director for Information Security, NSA.

THIS PAGE INTENTIONALLY LEFT BLANK